Amendments To Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A decryption device comprising:

an internal-key storage section adapted to store an internal-key;

a content-key storage section adapted to store content-keys;

a determination section adapted to determine whether or not a value of the content-key storage section in its initial state and a current value of the content-key storage section are different; and

an operation section, the operation section including:

a first decrypting section adapted to, when an encrypted content-key is input to the operation section, decrypt the encrypted content-key using the internal-key so as to obtain a content-key and store the content-key in the content-key storage section, and

a second decrypting section adapted to, when an encrypted content is input to the operation section and the determination section determines that the value of the content-key storage section in its initial state and the current value of the content-key storage section are different, decrypt the encrypted content using the current value of the content-key storage section as the content-key so as to obtain a first output data and output the first output data to outside of the decryption device,

wherein the determination section comprises a register for storing a value of the content-key storage section at the time that said register receives a Power On Reset (POR) signal, and

wherein the POR signal is a signal which pulses only once immediately after power-on or immediately after reset, so that the content key storage section is in an initial state immediately after ~~at least one of~~ a corresponding power-on or reset of the decryption device ~~and the decryption device is reset~~.

2. (cancelled)

3. (previously presented) A decryption device according to claim 1, further comprising a mutual authentication section adapted to determine whether or not a mutual authentication has been made between the mutual authentication section and a storage device which is located

outside the decryption device, and store the encrypted content-key being stored in the storage device;

wherein the second decrypting section is adapted to decrypt the encrypted content when the mutual authentication section determines that the mutual authentication has been made.

4. (previously presented) A decryption device according to claim 1, wherein:

the internal-key storage section is adapted to store a plurality of internal-keys; and

the internal-key storage section is adapted to select one of the plurality of internal-keys as the internal-key based on internal-key selection information input from outside the decryption device to the decryption device.

5. (previously presented) A decryption device according to claim 1, wherein:

the second decrypting section is further adapted to prevent decryption of the encrypted content when the determination section determines that the value of the content-key storage section in its initial state and the current value of the content-key storage section are the same.

6. (currently amended) A method for decrypting encrypted content in a decryption device including an internal-key storage section and a content-key storage section, the method comprising:

storing an internal-key in the internal-key storage section;

storing content-keys in the content-key storage section;

determining whether or not a value of the content-key storage section in its initial state and a current value of the content-key storage section are different; and

decrypting an encrypted content-key provided to the decryption device by using the internal-key so as to obtain a content-key and storing the content-key in the content-key storage section; and

when it is determined that the value of the content-key storage section in its initial state and the current value of the content-key storage section are different, decrypting the encrypted content using the current value of the content-key storage section as the content-key so as to obtain a first output data and outputting the first output data to outside of the decryption device,

wherein, for the determination step, a register stores a value of the content-key storage at the time that said register receives a Power On Reset (POR) signal, and

wherein the POR signal is a signal which pulses only once immediately after power-on or immediately after reset, so that the content key storage section is in an initial state immediately after ~~at least one of~~ a corresponding power-on or reset of the decryption device ~~and the decryption device is reset~~.

7. (cancelled)

8. (previously presented) A method according to claim 6, further comprising:

storing a plurality of internal-keys in the internal-key storage section; and

selecting one of the plurality of internal-keys as the internal-key based on internal-key selection information input from outside the decryption device to the decryption device.

9. (previously presented) A method according to claim 6, further comprising:

preventing decryption of the encrypted content when it is determined that the value of the content-key storage section in its initial state and the current value of the content-key storage section are the same.